O365 Terms of Use Agreement

SMARTER TOGETHER

Terms of Use Agreement for Microsoft Office 365 Cloud Services

These terms of use apply to HSE employees and any other persons who have been granted user rights to the Office 365 (O365) services by the HSE. O365 services include O365 mail (email), MS Teams, SharePoint, OneDrive, Planner, Forms, Power BI.

1.HSE Policies + legislation
This Terms of Use agreement should be read and construed with all existing HSE policies, rules and requirements, including the HSE data protection policy, HSE IT policies and the HSE Record Retention policy as well as Data Protection and Freedom of Information legislation. For information on the legislative framework for the processing of personal data in the HSE see here.

2.Acceptance
The misuse of HSE O365 services could pose a risk to the HSE. It is your responsibility to ensure you read, understand and comply with this Terms of Use agreement, along with HSE data protection policy, HSE IT policies and the HSE Record Retention policy. It is your responsibility to ensure that data is shared only for valid HSE operational and service delivery purposes; any users failing to comply with this *Agreement* and the HSE policies may be subject to HSE disciplinary procedures. You are deemed to have agreed to these Terms of Use by use of any O365 service e.g. O365 mail.

3.Business related purposes: O365 tools should only be used for HSE business related purposes. Personal information should not be stored or exchanged using O365 tools as set out in the HSE IT Acceptable Usage Policy and the HSE Electronic Communication policy

4.Monitoring: The HSE reserves the right to routinely monitor, log and record all use of the HSE O365 services for specific purposes e.g. preventing, detecting and minimising inappropriate use. For further details, see the HSE Electronic Communication policy

5.Data access requests: All data in O365 service is subject to Data Access and Freedom of Information requests under HSE data protection policy, and Freedom of Information and data protection legislation.

6.Record retention: Users are responsible ensuring that the legally mandated retention period requirements for records as set out in the HSE Record Retention policy are met. No O365 application location should be used in lieu of an appropriate permanent record repository.

Content in HSE O365 applications will be retained for a minimum of 7 years.

7.Guests:
A guest is an employee or contractor of a third-party organisation. Guests can only be enabled with access to HSE O365 services e.g.MS Teams where significant and on-going document collaboration is required. Where guest access is required, the team owners must ensure that the proposed third-party organisation must complete and sign appropriate HSE Data agreement(s). Guests will be removed from non-compliant teams where agreements are not completed. Guests cannot use personal email addresses e.g. Gmail/Hotmail

8.0365 Team/Group Owner Responsibilities:

- Ensure there are at least 2 and no more than 4 active owners for the Teams site/group
- Add and remove team members as needed
- Ensure that data and sharing information is managed in compliance with HSE IT policies
- Delete team/group when it is no longer required

9.Owner; guest access responsibilities:
Add and remove guest members as required, ensuring that:

- the type of data to be shared has been reviewed
- the type of third-party data will be shared with has been considered and
- the correct data agreement(s) are completed by the third-party provider organisation

10.HSE Data Types and Data Agreements
The type of HSE agreement required depends on:

- the type of third party that HSE data is to be shared with
- the type of HSE data to be shared

Types of third party:

Commercial Service Provider

If you are sharing HSE data with a *commercial service provider (i.e. individuals, companies and organisations providing information systems and support, consultancy services or data management service(s) to the HSE*, and as such acting as a “Data Processor” on behalf of the HSE) then the commercial service provider would need to sign copies of the following HSE documentation:

a) **HSE Service Provider Data Processing Agreement (Version 2.0);**
b) **HSE Third Party Network Access Agreement;**
c) **HSE Supplier IT Security Assessment Questionnaire.**

Government Dept. or Agency

If you are sharing HSE data with another *government department or agency, HSE funded agency or international governmental organisation* who will process the HSE data for their own statutory or other legal purposes, then the government department or agency, HSE funded agency or international governmental organisation would need to sign copies of the following HSE documentation:

a) **HSE Data Sharing Agreement;**
b) **HSE Third Party Network Access Agreement (HSE Funded Agencies).**

11.Sharing data with Third Parties outside Europe

In addition to the above HSE agreements and documentation, if you are sharing HSE **personal data** with any third parties who are based in a country outside the European Economic Area (EEA) which is not covered by an EU adequacy decision, there are additional legal agreements and risk assessments that **must** be signed and undertaken before you can share any HSE personal data. For assistance on queries concerning these providers, please contact the HSE Data Protection Office (DPO). See here for DPO contact details.

Types of data:

- **'Personal' is** defined under GDPR- see here for a short explanation.
- **'Confidential', 'Restricted'** are defined in the HSE Information Classification and Handling Policy

Please e-mail O365.Support@hse.ie for further information or queries.

In additional to the above agreements, the sharing of personal data may require the undertaking of a Data Protection Impact Assessment (DPIA). For assistance on whether or not a DPIA is required please contact the HSE Data Protection Office (DPO). See here for DPO contact details.

Summary – agreements required for guest access

What information is being shared with whom?	HSE Third Party Network Access Agreement	HSE Service Provider Data Processing Agreement	HSE Supplier IT Security Assessment Questionnaire	HSE Data Sharing Agreement	HSE Third Party Network Access Agreement (HSE Funded Agencies version)
Non-personal, non-confidential and non-restricted information with any third party	✓				
Personal, confidential, or restricted HSE information with a commercial service provider	✓	✓	✓		
Personal, confidential or restricted HSE information with another government department or agency, HSE funded agency or international governmental organisation				✓	✓
Personal, confidential or restricted HSE information with a third party based in a country outside European Economic Area (EEA)	Additional legal agreements and risk assessments must be signed. Contact with the HSE Data Protection Officer (DPO) is required. See here for DPO contact details.				

12.O365- information sharing

Sharing with HSE staff

Confidential and restricted information stored within the HSE O365 service must only be shared by you with other HSE staff who have a valid HSE business related reason and are authorised to have access to the information.

Sharing with general public

Confidential and restricted information stored within the HSE O365 services must only be shared by you with the general public in accordance with the relevant legislation and agreed HSE procedures (for example, *Freedom of Information Act 2014 / Data Protection Act 2018, / the General Data Protection Regulation 2016/679 (the "GDPR")*).

Sharing with third parties

Confidential and restricted information stored within the HSE O365 services must only be shared by you with third parties in accordance with the relevant legislation (for example, *Freedom of Information Act 2014* / *Data Protection Act 2018, / the General Data Protection Regulation 2016/679 (the "GDPR") / Health (Provision of Information) Act 1997 / Health Acts 1947 to 2007 etc*) and the HSE I.T. policies.

Record of agreement

Should you decide to share confidential or restricted information via the HSE O365 services with an external third party, **you** will be responsible for (1) ensuring the external third parties have signed the appropriate HSE agreements and related documentation **prior** to sharing any information with them, (2) retaining signed copies of these HSE agreements and documentation, and (3) making these HSE agreements and documentation available for audit.